Cisco Security Advisory

Cisco Nexus Dashboard Configuration Backup REST API Unauthorized Access Vulnerability

Medium

Advisory ID:
cisco-sa-nd-cbid-5YqkOSHu

First Published:
2026 April 1 16:00 GMT

Version 1.0: Final

Workarounds: No workarounds available

Cisco Bug IDs:
CSCwq66302

CVE-2026-20042

CWE-295

CVSS Score:
Base 6.5

Download CSAF

Email

Summary

A vulnerability in the configuration backup feature of Cisco Nexus Dashboard could allow an attacker who has the encryption password and access to Full or Config-only backup files to access sensitive information.

This vulnerability exists because authentication details are included in the encrypted backup files. An attacker with a valid backup file and encryption password from an affected device could decrypt the backup file. The attacker could then use the authentication details in the backup file to access internal-only APIs on the affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system as the *root* user.

Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

This advisory is available at the following link:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nd-cbid-5YqkOSHu

Affected Products

Vulnerable Products

At the time of publication, this vulnerability affected Cisco devices if they are running a vulnerable release of Cisco Nexus Dashboard, regardless of device configuration.

For information about which Cisco software releases were vulnerable at the time of publication, see the Fixed Software section of this advisory. See the Details section in the bug ID at the top of this advisory for the most complete and current information.

Products Confirmed Not Vulnerable

Only products listed in the Vulnerable Products section of this advisory are known to be affected by this vulnerability.

Cisco has confirmed that this vulnerability does not affect the following standalone products:

- Nexus Dashboard Fabric Controller (NDFC)
- Nexus Dashboard Insights
- Nexus Dashboard Orchestrator (NDO)

Note: Starting in Cisco Nexus Dashboard version 3.1(1k), the unified Nexus Dashboard software image includes the products in the preceding list. As part of the unified image, these products are affected and are fixed in fixed releases of Cisco Nexus Dashboard. See the Fixed Software section of this advisory.

Workarounds

There are no workarounds that address this vulnerability.

Fixed Software

Cisco considers any workarounds and mitigations (if applicable) to be temporary solutions until an upgrade to a fixed software release is available. To fully remediate this vulnerability and avoid future exposure as described in this advisory, Cisco strongly recommends that customers upgrade to the fixed software indicated in this advisory.

Fixed Releases

At the time of publication, the release information in the following table was accurate. See the Details section in the bug ID at the top of this advisory for the most complete and current information.

The left column lists Cisco software releases, and the right column indicates whether a release was affected by the vulnerability that is described in this advisory and which release included the fix for thi

vulnerability.

Cisco Nexus Dashboard Release	First Fixed Release
3.2 and earlier	Migrate to a fixed release.
4.1	Migrate to a fixed release.
4.2	Not vulnerable.

The Cisco Product Security Incident Response Team (PSIRT) validates only the affected and fixed release information that is documented in this advisory.

Exploitation and Public Announcements

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

Source

This vulnerability was found during internal security testing.

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nd-cbid-5YqkOSHu

Revision History

Version	Description	Section	Status	Date
1.0	Initial public release.	-	Final	2026-APR-01

Legal Disclaimer

SOFTWARE DOWNLOADS AND TECHNICAL SUPPORT
The Cisco Support and Downloads page on Cisco.com provides information about licensing and downloads. This page can also display customer device support coverage for customers who use the My Devices tool. Please note that customers may download only software that was procured from Cisco directly or through a Cisco authorized reseller or partner and for which the license is still valid.

Customers who purchase directly from Cisco but do not hold a Cisco service contract and customers who make purchases through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should obtain upgrades by contacting the Cisco Technical Assistance

Center (TAC). Customers should have the product serial number available and be prepared to provide the URL of this advisory as evidence of entitlement to a free upgrade.

When considering software upgrades, customers are advised to regularly consult the advisories for the relevant Cisco products to determine exposure and a complete upgrade solution. In all cases, customers should ensure that the devices to be upgraded contain sufficient memory and confirm that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, customers are advised to contact the Cisco Technical Assistance Center (TAC) or their contracted maintenance providers.

Copies or summaries of the information contained in this Security Advisory may lack important information or contain factual errors. Customers are advised to visit the Cisco Security Advisories page for the most recent version of this Security Advisory. The Cisco Product Security Incident Response Team (PSIRT) assesses only the affected and fixed release information that is documented in this advisory. See the Cisco Security Vulnerability Policy for more information.

▶ Cisco Security Vulnerability Policy

▶ Subscribe to Cisco Security Notifications

▶ Related to This Advisory